Software Verification and Validation Plan – Basic Phase

November 8, 2010

ASCEM-PM-QA/VV-110810-Rev. 01

ASCEM

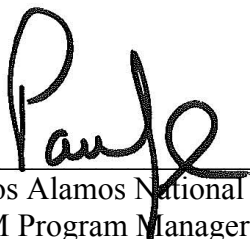**United States Department of Energy**

E_M Environmental Management

safety ❖ performance ❖ cleanup ❖ closure

Approval:

_____   ____11/08/2010____
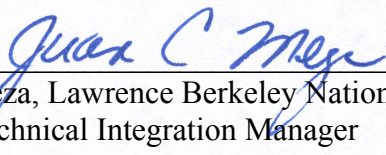Dr. Paul Dixon, Los Alamos National Laboratory   Date
Multi-Lab ASCEM Program Manager

_____   ____11/08/2010____
Dr. Juan Meza, Lawrence Berkeley National Laboratory   Date
ASCEM Technical Integration Manager

Concurrence:

_____   ____11/08/2010____
Ronald Schrotke, Jr., Pacific Northwest National Laboratory   Date
ASCEM Project Quality Engineer

Table of Contents

Tables

Figures

1.   INTRODUCTION

This document describes the verification and validation (V&V) processes that will enable the Advanced Simulation Capability for Environmental Management (ASCEM) team to maintain control of all work products during the ASCEM Basic, Applied, and Implementation phases (see the ASCEM Project Quality Assurance Plan [PrQAP] for discussion on phases). The verification and validation concepts that will be adopted by ASCEM include reviews, audits and testing.

1.1. *Scope*

As with other ASCEM software quality tasks, a risk-based graded approach is appropriate. What this means in practice is that the rigor to invoke for the verification and validation processes will be a function of whether the ASCEM work products are being developed for the Basic, Applied or Implementation phases. Section 4.1 discusses the risk-based graded approach (RBGA) for ASCEM verification and validation.

This Plan uses a tailored IEEE Std 1012-1998[1] as a guide to ensure that the salient V&V topics are addressed.

1.2. *Terms*

1. **Baseline** – A specification or product that has been formally reviewed and agreed upon, that thereafter serves as the basis for further development, and that can be changed only through formal change control procedures [1].

2. **Code Coverage –** A measure of the statements within a program that have been tested; i.e., the percentage of total program statements tested (C0 testing) or the percentage of statements including branches and loops that have been tested (C1 testing).

3. **Configuration Management** – A discipline applying technical and administrative direction and surveillance to a) identify and document the functional and physical characteristics of a configuration item, b) control changes to those characteristics, c) record and report change processing and implementation status, and d) verify compliance with specified requirements [1].

4. **Domain Expert** – A person who has special knowledge or skills in a particular area of interest.

5. **Functional Configuration Audit (FCA**) – An audit conducted to verify that the development of a configuration item has been completed satisfactorily, that the item has achieved the performance and functional characteristics specified in the functional or allocated configuration identification, and that its operational and support documents are complete and satisfactory [1].

---

1. IEEE Std 1012-1998, IEEE Standard for Software Verification and Validation

6. **Independent** – the quality requirement that reviewers do not either supervise or manage the resources (money and people) associated with the development and maintenance of any of the ASCEM software work products being reviewed.

7. **Open Source (& Gnu Software) –** Software that is provided free of charge.

8. **Physical Configuration Audit (PCA)** – An audit conducted to verify that a configuration item, as built, conforms to the technical documentation that defines it [1].

9. **Requirements Traceability Matrix (RTM)** – A matrix that records the relationships between products of the development process (e.g., a matrix that records the relationship between the requirements and the design of a given software component, between a design component and the source code for a module, and between the source code and test cases) [1].

10. **Risk-Based Graded Approach (RBGA) –** A DOE mandated approach that means the process of ensuring that the level of analysis, documentation, and actions used to comply with a requirement are commensurate with:

    • The relative importance to safety, safeguards, and security (Level of Risk)

    • The magnitude of any hazard involved

    • The relative importance of radiological and non-radiological hazards

    • Any other relevant factors.

11. **Software Quality Engineering (SQE) –** The integration of quality, reliability, safety, and software engineering to address process control and design improvement.

12. **Subject Matter Expert (SME**) – a person who is an expert in a particular area or topic.

13. **Verification –** The process of evaluating a system or component to determine whether or not the products of a given development phase satisfy the conditions imposed at the start of that phase [1].

12. **Validation –** The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements [1].

13. **Work Product** – Any artifact produced by a process, including files, documents, parts of the product, services, processes, specifications, and invoices.

2. ORGANIZATION

Figure 1 below outlines the ASCEM organizational structure. The software quality and other associated quality processes (such as configuration management and V&V responsibilities) are allocated across the ASCEM organizational matrix.
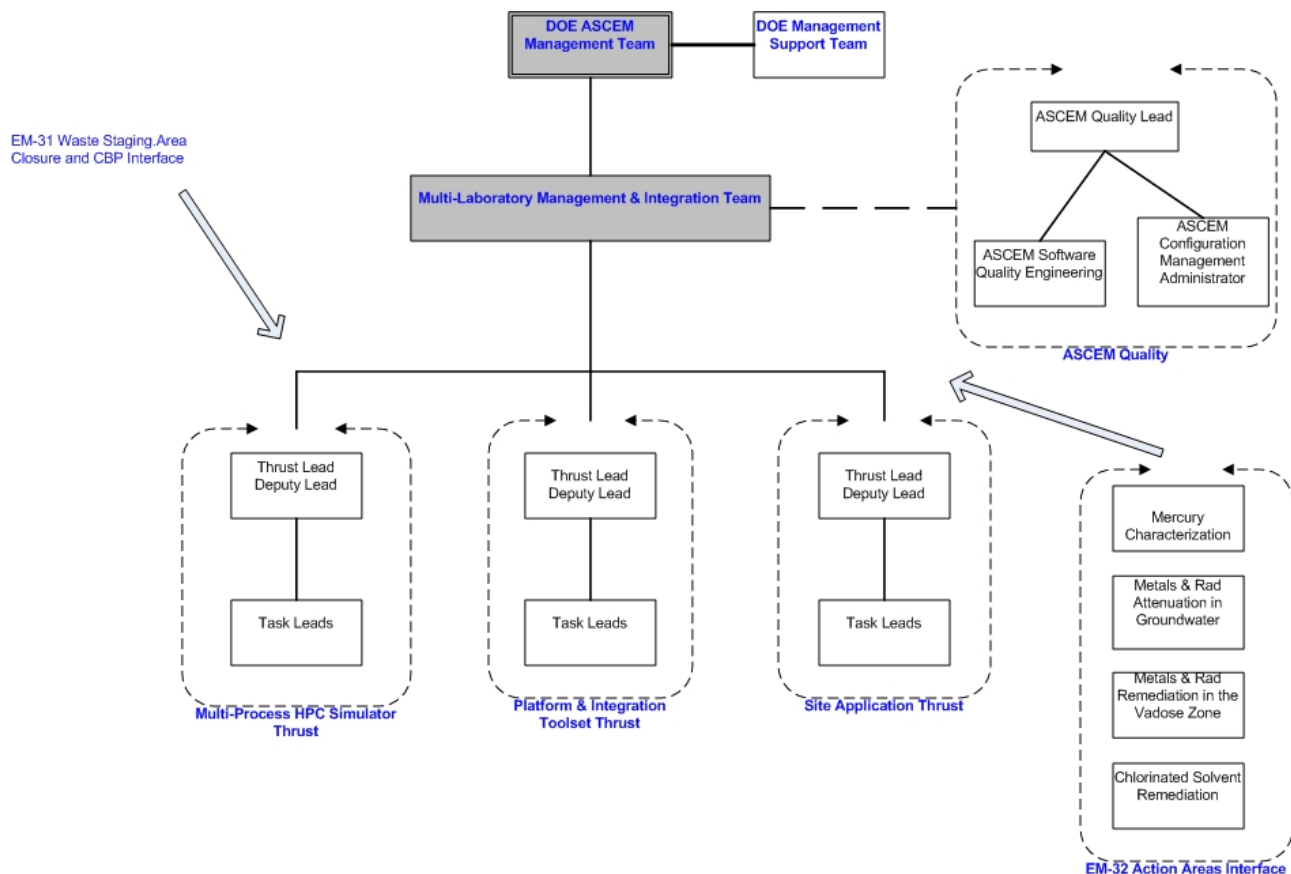

Figure 1. ASCEM Organization.

2.1. Responsibilities

Responsibilities delineated below maybe filled by the same person.

2.1.1. ASCEM Change Control Board

ASCEM Baseline Management, Risk and Change Control Directive, July 1, 2010, addresses the change control process and will not be replicated herein.

2.1.2. ASCEM Program Manager

The ASCEM Program Manager assures that the "job is being done right" and that "the right job is being done." The ASCEM Program Manager must develop and deliver an ASCEM system designed against the requirements, coded against the design, and tested against the code. Similarly, the ASCEM Program Manager must assure that the final ASCEM system application satisfies its customer requirements in its target environment while not performing any unintended or adverse functions.

2.1.3. ASCEM Quality Lead

The ASCEM Quality Lead ensures that the ASCEM system is compliant with the NQA-1-2004[2] Nuclear Quality Assurance criteria, as well as invoking appropriate software quality processes during the development and deployment of ASCEM modules.

2.1.4. ASCEM Software Quality Engineering Lead

The ASCEM Software Quality Engineering Lead creates/develops all software quality engineering work products and reviews those work products to assure their robustness and integrity. The ASCEM Software Quality Engineering Lead also assures compliance with NQA-1.

2.1.5. ASCEM Thrust Leads

The ASCEM Thrust Leads ensure that all the work products under their purview have appropriate configuration identifiers assigned, and are appropriately managed.

3. RELATIONSHIP OF THIS V&V PLAN WITH OTHER ASCEM QUALITY DOCUMENTS

The authority and requirements for this ASCEM Verification and Validation Plan are derived from the superordinate documents as noted in the document hierarchy diagrammed in *Figure 2* on the next page. Consequently, if there are any disagreements within or among the quality assurance (QA) artifacts supporting ASCEM, the higher tier document has precedence. Thus, all the risk-based quality assuring and V&V processes mandated within the higher tier ASCEM software quality documents must be invoked within this document to be compliant.

---

2. ASME NQA-1-2004 (including addenda 2005 and 2007), Subpart 2.7 (*Quality Assurance Requirements for Computer Software for Nuclear Facility Applications*), and 4.2 (*Guidance on Graded Application of Quality Assurance for Nuclear-Related Research and Development*).
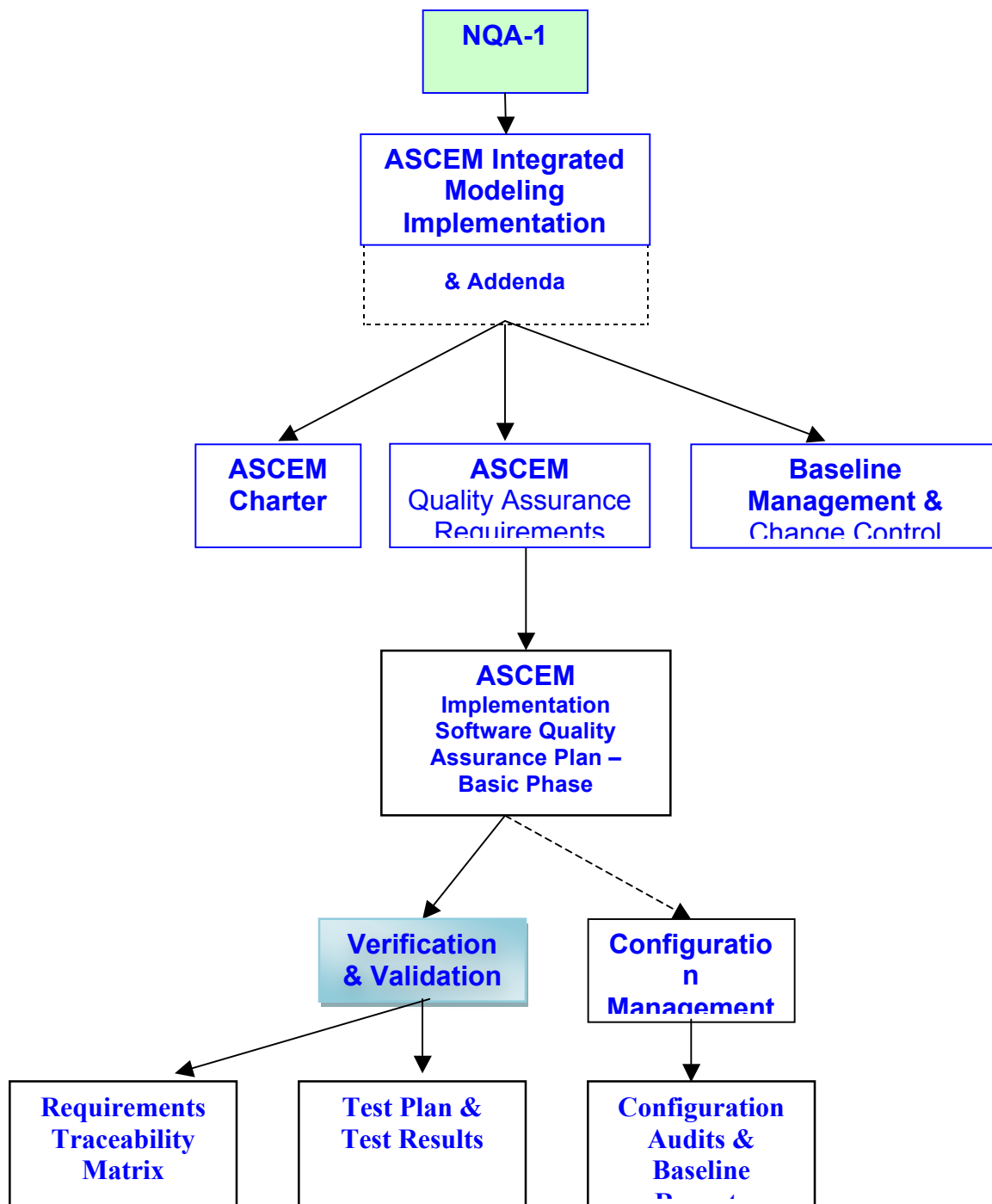
Figure 2. Relationship of software quality plans to other ASCEM documents.

4.   VERIFICATION AND VALIDATION ACTIVITIES

4.1. *A Definition for Risk-Based Graded Approach for ASCEM Verification and Validation*

Since an RBGA is appropriate for managing all ASCEM software QA activities, the following software QA activities are applicable for the Basic Phase:

- Configuration management insofar as configuration identification and version control
- High-level software requirements definition
- Documentation of functionality for prototype or agile developed application
- Documentation for software testing and test results.

Additional RBGA rigor will be required for the succeeding Applied and Implementation phases. As the Applied Phase transitions to the Implementation Phase, increased rigor will be required around the safety software requirements.

4.2. *Reviews and Audits*

Reviewing and auditing are vital linchpins of V&V; they discover errors more effectively than just testing. In addition, since reviews can occur earlier in the software development life cycle, they are more cost effective. As with other V&V elements, the approach for reviews and audits should be risk-based. The table below lists which reviews and audits to implement for the Basic Phase. Note that the reviewers for all phases must be *independent*.

Table 1. *Recommended Reviews for Basic Phase.*

Phase	V&V Sections To Address
Basic	4.2.1: Requirements Review 4.2.2: Test Plan & Acceptance Test Plan 4.2.3: Functional Configuration Audit 4.2.3: Requirements Traceability Matrix

4.2.1. Requirements Review

Reviews of all the ASCEM software requirements are critical to ensure requisite correctness, completeness, and verifiability. Software requirements reviews must involve both domain experts and software quality engineers.

Domain SMEs must evaluate whether the proposed functionality and algorithms are correct and viable for the application. Part of this task will be to evaluate the stated parameters for correct

data ranges and anomaly management. Without at least a basis for anomaly management, any transition of the ASCEM application(s) to a safety software application will not be effective.

Reviews by SQEs will support the assessment of whether the documented requirements will support verifiability and thus permit both design and testing. The SQE will assess whether the requirements are ambiguous or not, and if the requirements documentation properly lists constraints, assumptions, quality attributes, and performance requirements.

4.2.2. Test Plan & Acceptance Test Plan Review

The Test Plan and the subordinate Acceptance Test Plans must detail the following:

- The test setup
- Initiation and test environment at initiation
- Test steps
- Expected outcome
- Contact personnel if any test steps fails
- The protocol if defects are discovered during the testing process.

This latter step must specify whether the tester should stop testing until the defect (whether due to an incorrect interpretation of the test case steps or because of a code defect) is resolved. The Test Plan review process must include domain SMEs, and SQEs. The inclusion of computer science parallel computing experts and human factor experts are at the discretion of the ASCEM Program Manager and the ASCEM Quality Lead.

4.2.3. Review of Legacy/Acquired/Third-Party Software

Another vital V&V activity is determining if legacy/Third-Party/acquired software and libraries provide the following:

- Necessary capabilities for intended use
- Limitations for intended use documented
- Test plans and test cases to demonstrate the capabilities within the defined limitations
- Instructions for use within the understood limits and constraints.

The Thrust Leads and their respective teams must make these determinations, in agreement with the QA and SQE Leads, as well as document the assessments and any associated risks.

4.2.4. Functional Configuration Audit

Conduct of a Functional Configuration Audit (FCA) is an essential V&V activity during the Basic Phase. The FCA ensures that the product and supporting documentation accurately record what functions/algorithms and behaviors are incorporated into ASCEM. All ASCEM Thrust

Leads and their teams must have confidence that ASCEM's functionality is known, understood, and behaves without "surprises." The SQE leader will provide ASCEM management and Thrust Leads with the documented FCA results.

4.2.5. Requirements Traceability Matrix

The Requirements Traceability Matrix is the primary, Basic Phase V&V activity to ensure that the ASCEM product was developed correctly and functions as intended while not performing any unintended functions.

4.3. Defect Tracking

The ASCEM Configuration Management Plan discusses the discovery of defects as a result of the development and testing process. This material will not be replicated herein.

4.4. Test V&V

4.4.1. Testing & V&V Tools

Software tools that could support the ASCEM V&V objectives include coverage analyzers (C1), and regression test.

There are many open source software tools (depending upon the target language and operational environment) available to support the developer and tester.

Appropriate automated testing tools to support the ASCEM platforms and project objectives will be investigated by the appropriate Thrust Leads and the SQE Lead.

4.4.2. Testing Process

Testing is an essential part of the final V&V process to ensure that "the right job is being done." Testing determines if the ASCEM application functions as intended within the target environment without performing any unintended or adverse functions.

Many tests only address nominal operational parameters. Although the tests must include the nominal cases, the Thrust Leads and ASCEM SQE must remember that the purpose of a software tests is to "break" the application before the user community obtains it and unhappily discovers that it does not perform as intended.

Table 2 below lists the minimum testing activities that are required for the Basic Phase. Reference the applicable sections for further information about these testing processes.

Table 2. *Minimum Testing Activities for Basic Phase.*

Phase	Testing Sections To Address
Basic	4.4.3: Thrust and Task Lead Team V&V 4.4.4: Usability Testing 4.4.5: Acceptance Testing

4.4.3. Thrust and Task Lead Team V&V

As the ASCEM application is being built, the Thrust and Task Leads may want to have another person on their team internally review and test it. During the builds for the units and the integration of the units into the module(s), testing will be essential to ascertain whether the application is satisfying the requirements and design expectations. These "build tests" typically test nominal values, but the team may also want to test anomalous events to ascertain if the appropriate error-handling paths and message dialogs were used.

The team may also want to perform additional rigorous testing that they perceive as beneficial.

4.4.4. Usability Testing

Usability testing addresses the "human factors" attributes of the ASCEM applications. Such attributes as screen colors, fonts, font colors, menu format and access, anomaly management, and ambient lighting in the operational environment should all be considered during usability testing. This testing is essential because it reflects probable use by the User Community.

4.4.5. Acceptance Testing V&V

Acceptance testing is the "turnkey" testing for the User Community to assure the users that all the ASCEM applications function as intended in their target environment. The Acceptance Test cases are merely an aggregation of specific test cases previously exercised for other specific purpose tests.

4.5. *Managing Baselines*

The ASCEM Configuration Management Plan discusses the management and release of a baseline, which results from a V&V process. This process will not be discussed herein.

5.   MAINTENANCE OF V&V PLAN

This ASCEM Software Verification & Validation Plan will be annually reviewed by the ASCEM Quality Lead to ensure that the described V&V processes are correct, complete and compliant with the mandated NQA-1-2004 quality criteria. If any changes are needed, the ASCEM Quality Lead will ensure that the necessary revisions are made, and submit the revised documents to ASCEM Program Management for approvals.

REFERENCES

[1]   IEEE 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology.
[2]   IEEE 1012-1998, IEEE Standard for Software Verification and Validation.

APPENDIX A - ACRONYMS AND ABBREVIATIONS

ASCEM	Advanced Simulation Capacity for Environmental Management
FCA	Functional Configuration Audit
NQA	Nuclear Quality Assurance
PrQAP	Project Quality Assurance Plan
QA	Quality Assurance
RBGA	Risk-Based Graded Approach
V&V	Verification and Validation
SME	Subject Matter Expert
SQE	Software Quality Engineering